Banque Internationale à Luxembourg
société anonyme
69, route d'Esch · L-2953 Luxembourg · Tél.: (+352) 4590-5000
R.C.S. Luxembourg B-6307 · BIC Code : BILLLULL
TVA : LU 11180925 · LEI Code : 9CZ7TVMR36CYD5TZBS50

Policy on the Processing of Personal Data

Banque Internationale à Luxembourg (hereinafter referred to as "**the Bank**" or "**BIL**"), acting in its capacity as data controller (i.e. determining the purposes and means of the processing of personal data), attaches the utmost importance to the protection of your personal data (i.e. any information relating to an identified or identifiable natural person).

The Personal Data Protection Policy (hereinafter, "**the Policy**") applies for all natural persons whose personal data are processed by BIL in the context of a business relationship, in accordance with Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, "the GDPR"). This Policy describes the Bank's obligations as data controller, the processing activities carried out, as well as your rights with regard to your personal data.

The Bank undertakes not to sell your personal data to any third party whatsoever.

1. Personal data processed

The personal data processed by the Bank may be supplied directly by you, collected by the Bank when you use the services, supplied by third parties or come from public sources.

In certain cases, refusing to communicate personal data to the Bank and prohibiting it from processing such data could prevent the Bank from providing certain products or services or prevent you from continuing a relationship with the Bank.

Any person who communicates to the Bank personal data relating to third parties (e.g. family members, close relations, agents, legal representatives, company shareholders, managers, directors or beneficial owners) must be authorised to do so by these third parties and must inform them that the Bank processes personal data for the same purposes and in accordance with the same procedures as those set out in this Policy.

For the purposes of fulfilling its obligations and as far as necessary, the Bank may process "special categories of data", such as data relating to health, convictions and offences and the exercise of a public function.

In the course of its activities, the Bank processes various categories of personal data depending on the services you have subscribed to or are about to subscribe to, as indicated below:

Personal data you provide to the Bank :

- Personal identification data: *e.g. gender, first name, surname, date and place of birth, nationality, signature specimen, etc. ;*
- Contact details: *e.g. telephone number, postal address, e-mail address, language of communication, etc;*
- Professional data: *e.g. function, salary, employer, etc. ;*
- Tax data: *e.g. tax identification number, tax status, etc. ;*
- Data relating to your family situation: *e.g. marital status, family members, etc. ;*
- Official documents: *e.g. copy of identity card, passport, residence permit, certificate of residence, etc. ;*
- Economic and financial data: *e.g. income, origin of funds, assets, etc. ;*
- Commercial data: *e.g. products subscribed, outstanding amounts, maturity dates, amounts, etc. ;*
- Data relating to your risk score: *e.g. for credit risk, investment services, etc.*
- Data relating to insurance: *e.g. insurance companies, types of insurance, amounts insured, etc. ;*
- Information about your projects;
- Data resulting from exchanges by electronic, postal or telephone means, or from exchanges in person.

Personal data collected by the Bank when you use its services :

- Connection and browsing data: *e.g. authentication method in BILnet, cookie preferences, IP address, actions carried out in BILnet;*
- Geolocation data: *e.g. when you ask to find your nearest branch on BILnet ;*
- Transaction data: *e.g. amount, date and time of transaction, currency, beneficiary and payer, place of transaction;*
- Video recordings from video surveillance systems installed in and around buildings and installations, including ATMs;
- Telephone recordings.

Personal data from third parties :

- Identification and contact details of third parties*: e.g. details of a beneficiary of a dormant or unclaimed account, details of an heir;*
- Data relating to criminal convictions and offences: *e.g. data from a database used to fight money laundering and the financing of terrorism;*
- Identification data, contact data and economic and financial data provided by third parties: *e.g. data on a beneficial owner provided by a company representative, account proxy;*
- All data from public authorities: *e.g. court orders, ad hoc requests from a regulatory authority.*

Personal data from public sources :

- Data from social networks: *e.g. to meet legal due diligence obligations;*
- Data from press articles;
- Data from online registers: *e.g. register of companies, register of beneficial owners.*

All the personal data mentioned above may be processed by the Bank for all individuals with whom it comes into contact in the context of a commercial relationship, depending on the services provided or about to be provided.

This includes, but is not limited to :

- Customers;
- Prospects ;
- Heirs and beneficiaries ;
- Instructing parties or beneficiaries of a payment instruction ;
- The guarantors ;
- Proxies or representatives, including notaries and lawyers;
- Beneficial owners of legal entities.

2. Data processing purposes and retention periods

The Bank only collects personal data that is necessary for the performance of the services provided to you and to comply with its legal obligations.

The personal data collected and processed by the Bank is used for various processing purposes, depending on the services to which you have subscribed or are about to subscribe. Once these purposes have been achieved, the Bank erases the said personal data. As an exception (legal interruption and suspension of retention periods), the Bank may retain data beyond the periods mentioned below, in compliance with the applicable legal provisions.

The main purposes and the resulting retention periods are as follows:

- Compliance with a legal obligation to which the Bank is subject:

- successful and unsuccessful entries into relationship;
- Directives on client information for investment services in the field of financial instruments (MiFID) and insurance products (IDD);
- customer identification to facilitate the exercise of voting rights in respect of listed European companies;
- reporting obligations and automatic exchange of information with the relevant authorities, whether in Luxembourg or not;
- the Bank's effective management of credit risk and your ability to repay, including the regular valuation of your property;
- verification of the payee's name during a payment instruction;
- detection of fraudulent transactions;
- prevention of market abuse;
- prevention of any attempt at fraud ;
- requests from local and foreign authorities;
- bookkeeping;
- management of non-performing loans;
- management of dormant accounts, estates, debt recoveries, insolvency proceedings, seizures, litigation, etc.
- audit assignments;
- complaints management;

- the recording of telephone conversations that give rise or are intended to give rise to transactions;
- obligations relating to compliance with the GDPR.

Personal data processed in order to comply with legal obligations is kept for 10 years after the end of your relationship with the Bank, except for the following processing activities, which have a different retention period :

Data processing	Data retention period
Failure to enter into a relationship	2 years after the last interaction
Recording of telephone conversations that give rise or are intended to give rise to transactions	10 years after the date on which the conversation was recorded
Litigation management	30 years after the conclusion of the litigation, depending on the situation provided for in the Civil Code
Management of dormant accounts	10 years after the transfer of assets to the Caisse de Consignation
Management of transactional documents	10 calendar years after the close of the financial year to which they relate

- The performance of a contract between the Bank and you or the performance of pre-contractual measures. In particular, personal data is processed for the setting up, administration and management of the contractual relationship and for updating your information for :

- the provision of banking and insurance services;
- the execution and recording your financial transactions;
- the definition of your credit risk score and your risk appetite in relation to the provision of investment services;
- the supply of your notices and account statements;
- the management of your credit applications;
- the management of your access to our BILnet online service;
- debt recovery.

Personal data processed as part of the performance of a contract is kept for 10 years after the end of your relationship with the Bank.

- Your consent collected for prospection and marketing purposes relating to banking, financial and insurance products, or to other products promoted by the Bank, as well as the management of analytical monitoring on BILnet.

Your consent is active until it is withdrawn, which can easily be done in your BILnet space. Marketing and commercial surveys that you receive by e-mail are deleted 90 days after the form is sent
Acceptance of analytical monitoring is requested every 12 months on BILnet.

- The performance of a **mission of public interest** to which the bank is subject :

- the fight against money laundering and the financing of terrorism, including applicable laws on international sanctions and embargoes;
- Know Your Customer" obligations

Personal data processed in the public interest is kept for 10 years after the end of your relationship with the Bank.

- The Bank's **legitimate interest in** :

- ensuring your safety, protecting the property for which it is responsible and preventing all kinds of incidents;
- providing quality services increasingly tailored to your needs;
- conducting satisfaction surveys and opinion polls;
- ensure the security of IT networks and information;
- issue internal reports and statistics as part of risk management and the improvement of the Bank's products and services;

- manage potential disputes and litigation.

Data processing	Data retention period
Video surveillance management	No later than 30 days after recording
Satisfaction surveys, opinion polls and requests for appointments	90 days after the form is sent

3. Profiling activities and automated decisions

As part of its activities and in order to serve you better, the Bank uses profiling and automated decisions. The profiling mechanism brings together a set of processing activities aiming to :

- collect and analyse information about your economic situation and your banking behaviour in order to assign you a profile and provide you with appropriate personalised commercial offers, including investment products that meet your risk profile;
- manage the risk to which the Bank is exposed by analysing your banking behaviour as well as by getting information about your financial situation and the risks posed by certain of your requests, such as a request to increase a credit limit;
- fighting fraud, money laundering and the financing of terrorism by analysing your profile, your geographical area, your banking habits and your transaction history against a set of predefined criteria to detect suspicious behaviour.

The Bank has automated certain decision-making processes to speed up the processing of requests and ensure impartiality :

- requests to change your credit card limits;
- managing overdrafts on your accounts ;
- blocking your credit cards if sufficient funds are not available;
- unblocking your credit cards as soon as the accounts are funded;
- adjustment of mortgage rates in the event of recurrent non-domiciliation of income.

The logic behind the decision is based on an analysis of your banking behaviour and of the assets and credits on your account.

In the context of these automated decisions, you have the right to request that the Bank re-examine your situation by means of the right to human intervention.

4. Data transfers and recipients

Certain personal data may be transmitted to certain recipients for whom the Bank has ensured the lawfulness and security of the transfer by means of technical and organisational security measures and/or binding legal instruments.

These recipients of personal data are required to comply with legal and contractual obligations relating to the protection of personal data, including professional secrecy or applicable confidentiality obligations.

Your personal data may be transferred by the Bank to the following categories of recipients in particular :

Recipients	Purposes of transferring personal data
Subsidiaries or branches of the Bank	BIL Lease: execution of a leasing contract signed by the customer BIL France: management of the business relationship with the customer.
External auditors	Carrying out audits of the Bank: auditing and certification of the Bank's accounts (in which case the auditor acts as data controller).
Lawyers and solicitors	e.g. in the event of debt recovery and extension of mortgage

Other financial institutions, including banks, insurance companies, tax experts, payment and credit card issuers, interbank messaging platform managers, online payment solution providers, etc.	All these institutions act as data controllers for the services and products offered by the Bank : - process a transaction on a financial instrument - offer an insurance product - provide a payment card - provide securities depository services - intervene in payment instructions - produce a tax report
Luxembourg tax authorities	Legal and regulatory obligations relating to the mandatory exchange of information in tax matters (CRS/FATCA) with countries that having signed up to it. The Luxembourg tax authorities may communicate the data transmitted by the Bank to any competent foreign tax authority pursuant to the applicable legal and regulatory obligations.
Administration de l'Enregistrement, des Domaines et de la TVA, Luxembourg	Legal obligation for the Bank to transmit payment information as part of the fight against VAT fraud.
Foreign supervisory authorities Companies issuing financial instruments Depositaries and sub-depositaries	In some jurisdictions, the legal and regulatory provisions applicable to (transactions involving) financial instruments and similar rights require that the identity of the (in)direct holders or beneficial owners of such instruments and their positions in such instruments be disclosed. Failure to comply with these requirements may result in the freezing of the financial instruments (with the effect, where applicable, that voting rights may not be exercised, dividends or other rights may not be received, and the financial instruments may not be sold or otherwise disposed of) or any other sanction or restrictive measure provided for by the aforementioned provisions. In the event of investment in this type of financial instrument, the customer must comply with the applicable legal and regulatory provisions. To this end, the customer expressly authorises the Bank to disclose, at its discretion, the identity of the customer and/or the beneficial owner and their positions in the said financial instruments.
Public authorities (e.g. judicial police, Cellule de Renseignement Financier (CRF), Commission de Surveillance du Secteur Financier (CSSF), etc.);	Responding to ad hoc requests from the authorities.

External service providers (the main external service providers are listed in the attached table)	The Bank uses external service providers: With regard to the services provided, in particular : - banking interfaces (account aggregation) - information technology (management and hosting of IT infrastructure) - physical security (cash in transit, video surveillance) - printouts (account statements, documents and letters) - management of customer documents and data (secure storage and destruction, quality review) - consultancy (e.g. development of new products and services) - communications (management of telephone and e-mail communications) - debt recovery All these service providers act as data processors of the Bank. Within the framework of the Bank's legal and regulatory obligations, in particular : - aiming to "get to know the customer" (through reports and research, in which case the service provider acts as data controller) - of identification of customers who are shareholders in European companies and facilitating the exercise of their voting rights (by sending position reports to European issuers and information on general assemblies sent to customers)
Other recipients	- on the basis of your instructions (consent) - by virtue of a legal or regulatory obligation

In principle, personal data is processed within the European Economic Area (EEA). However, certain data processing activities carried out outside the EEA by a service provider or a subsidiary. In such cases, before transferring any data whatsoever, the Bank ensures that, depending on the situation :

- The country to which the data is transferred benefits from an adequacy decision issued by the European Commission;
- The recipient of the data has put in place appropriate safeguards, such as standard contractual clauses for data transfers to third countries.

In these exceptional cases, and for the processing of personal data that is not repetitive, the Bank may transfer personal data to third countries without appropriate safeguards (e.g. transfer of data to a third country in the context of a dispute with a customer abroad).

5. Security of your data

The Bank undertakes to take all the technical and organisational measures necessary to guarantee the confidentiality, integrity and availability of your personal data. To this end, the following non-exhaustive measures are implemented to ensure the security of your data :

- Information and training of the Bank's staff on their data protection obligations;
- Rigorous application of data protection principles by design and by default for all products, services and functions offered by the Bank;
- Implementation of an information security framework ;
- Strict application of internal procedures and policies;

- The contractual obligation that the Bank's subcontractors offer and implement a similar level of data protection, in accordance with the General Data Protection Regulation (GDPR).

6. Exercising your rights

In accordance with the provisions of the GDPR, you may exercise the following rights :

- Right of access to your personal data;
- Right to rectification of your personal data;
- Right to erasure of your personal data under the conditions and within the limits of the Bank's legal and contractual obligations;
- Right to limit the processing of your personal data;
- Right to the portability of your personal data ;
- Right to object to the processing of your personal data
- Right to object to automated decision-making

With regard to processing activities based on automated decision-making, the right to human intervention may be exercised for all processing operations concerned, with the exception of the processing activities :

- Based on the performance of a contract ;
- Consent-based ;
- Which automated decision-making is legally authorised.

If the legal basis for processing is your consent, you may give or withdraw your consent at any time (Opt-Out). Withdrawal of consent does not compromise the lawfulness of processing based on consent carried out prior to the withdrawal.

For processing linked to marketing or commercial prospecting, you can change your consent directly in your BILnet space.

All the above rights can be exercised through various communication channels :

- By secure message on BILnet, by sending your request to the Bank's Data Protection Officer ;
- By e-mail to the following address: dpo@bil.com ;
- Via the dedicated form available on our bil.com website under the following link : https://survey.bil.com/?e=328967&d=l&h=7FB269DAC3609B7&l=en
- By post to the following address
  Banque Internationale à Luxembourg S.A.
  For the attention of the Data Protection Officer
  69 route d'Esch
  L-2953 Luxembourg

The Bank will endeavour to reply as soon as possible, and at the latest within one month of receiving your request. Depending on the complexity of the request, this deadline may be extended by two months. The Bank will inform you of this extension and the reasons for the postponement within one month of receiving the request. Certain exercise requests may be subject to limitations. Legal obligations may oblige the Bank not to give effect to the right to be forgotten (erasure). Requests for access may be limited in order to protect the rights and freedoms of others.

In the event of a request that is manifestly unfounded or excessive, the Bank reserves the right to demand payment of reasonable fees that take into account the administrative costs incurred in providing the information, making the communications or taking the measures requested. Any request will be deemed excessive from the 3rd request to exercise the same right made during the rolling year following receipt of the first request. The Bank may then demand payment of fees equivalent to the search costs defined in its price list available on bil.com.

If you receive an unsatisfactory reply, you can lodge a complaint with the National Commission for Data Protection (CNPD):

- Either by post to the following address: 15, Boulevard du Jazz, L-4370 Belvaux ;
- Or online on cnpd.lu in the "Individuals" section -> "Asserting your rights".

You can file a complaint with the competent supervisory authority, which is the authority for your country of residence.

Appendix: Table of main service providers

The Bank mainly uses the following external service providers for subcontracting purposes, in particular to process the following personal data :

Service provider	Purpose	Geographical area of processing
Bosch Germany	Video surveillance management	Germany
Medallia (formely. CheckMarket Belgium)	Management of mailings and satisfaction surveys	Belgium
POST Telecom S.A. Luxembourg	Management of telephone recordings	Luxembourg
Isabel S.A. (Multiline) Belgium	Payment Services	Luxembourg
kyndryl Luxembourg (PSF)	Provision of IT services	Luxembourg and Poland
i-Hub Luxembourg (PSF)	Centralisation and pooling of KYC data	Luxembourg
Lab Luxembourg (PSF)	Archiving of electronic signatures	Luxembourg
LexisNexis United-Kingdom	Customer information research	Ireland
Luxhub Luxembourg (PSF)	• Issuance of the CESOP report; • Verification of the payee's name; • Execution of Instant Payments.	Luxembourg
LuxTrust Luxembourg (PSF)	Issuing and management of digital identities (LuxTrust certificate)	Luxembourg
Microsoft Ireland	Provision of the Microsoft 365 service to the Bank	European Union
Payconiq Luxembourg	Provision of the Payconiq service	Luxembourg
Salesforce Ireland	Supply of the Bank's CRM Relationship management Secure messaging management	Sweden
Snowflake Netherlands	Large-scale calculation, data manipulation and analytical exploitation	Netherlands, Germany
SWIFT Belgium	Secure message exchange for financial transactions	Netherlands
Twilio United States	Sending of anti-fraud texts when logging in to BILnet or i-Hub	United States
Victor Buck Services Luxembourg (PSF)	Printing and mailing management	Luxembourg
Worldline Financial Services Europe S.A. Luxemburg (PSF)	Card editing/personalization Issuer processor activities Card blocking, incidents and dispute management Management of the 3D Secure function	Luxembourg